RECEIVED
CENTRAL FAX CENTER

JAN 16 2007

REMARKS

Claims 1-21 are pending in the application.

Claims 1-21 stand rejected under 35 U.S.C. 9102(b) as being anticipated by Michelle L. Hankins, SIGNAL AFCEA'S International Journal, October 1999 "Integrated Circuit Chip Provides Secure, Rapid Data Encryption" ('Hankins').

Applicants respectfully submit that there is nothing enabling in the Hankins article. Hankins is not an inventor, but merely the author of an article that very generally describes the work of the Applicants in an area adjacent to the present invention. Hankins is only reporting on the existence of a pipelined, key-agile ASIC to perform high speed encryption using the DES algorithm. The device described in the Hankins article requires the present invention to operate at its fullest potential; it does not provide the advantages of the present invention.

Unlike the present invention, the device described in the Hankins article is only capable of the use of non-feedback modes of operation. This limitation is unstated in the Hankins article. But the Applicants, having provided the information contained in the Hankins article, are aware of the limitations of the devices described in the Hankins article. This limitation means that the full operating rate (predicated upon keeping the pipeline full) is based on non-feedback modes of operation, such as Electronic Code Book (ECB) mode or Counter Mode (CM). When the device described in the Hankins article is used with a mode of operation requiring feedback around the encryption/decryption engine, as provided by the present invention, such as Cipher Block Chaining (CBC) mode, the throughput drops drastically. In testing, the Applicants observed that the data throughput rate for the Hankins-described DES ASIC operating in

CMC mode dropped from the 6.7 billion bits per second stated in the article to about 373 million bits per second. Cascading three (3) of these ASICs, as described in the Hankins article, to implement Triple DES with the CBC mode of operation further decreased the observed throughput to about 124 million bits per second. The theoretical maximum of 9.28 billion bits per second stated in the Hankins article was reduced to about 515 million bits per second and 172 million bits per second, respectively, for DES and Triple DES when using the CBC mode of operation or other modes of operation involving feedback.

The methods presented in the present application enable the DES ASIC referenced by Hankins (and other similarly designed encryption/decryption chips) to be used at their full rate, **even when used with modes of operation requiring feedback**, by gathering data from many security contexts and interleaving them through the pipelined encryption chip. At the decryption end, the data is distributed to the appropriated applications, as determined by the security context. This can keep the pipeline full and the encryption/decryption engine productively busy by processing data blocks from other security contexts, so it does not have to pause and wait for the data block from a particular security context to be processed and fed back before it can proceed with the next block. The Hankins article only addresses using non-feedback modes of operation, which can naturally keep the pipeline full, and writes nothing about the well-known problem of having to wait (run the pipeline dry or "flush the pipeline") for the required block when using a mode of operation involving feedback around the encryption/decryption engine. Therefore, Hankins is not enabling.

Regarding the specific claim rejections, Hankins does not teach how to use the DES ASIC or a similar device to its fullest extent when the practitioner or system

designer wishes to employ an encryption mode of operation that requires a feedback loop around the encryption/decryption engine, such as CBC mode. Hankins does not disclose or teach anything about feedback (around the pipeline stages), encryption context identifiers, or a bank of variables (comprising initial variables, and/or output from previous encryption/decryption stages). Hankins does not discuss these concepts at all. Hankins doesn't describe the need for, or the use of, an entire bank of initial or feedback variables, or indexing into such a bank. Hankins doesn't even hint that to avoid running the pipeline dry, you must have at least as many security contexts as there are pipelined encryption/decryption stages. Hankins does not tell how to use the Sandia DES ASIC or any other encryption/decryption chip in ANY mode of operation. Hankins doesn't even mention encryption/decryption modes of operation or the standards (FIPS PUB 81, ANSI X3.106, ANSI X9.52) that define them. The present invention teaches all of this.

It should also be pointed out that the claims are worded with terms as "an encryption/decryption process such as Data Encryption Standard (DES)," not limiting these submitted methods to a particular cryptographic algorithm, but using that algorithm to illustrate the class of algorithms for which these methods are applicable.

ATTORNEY DOCKET NO. SD-6769.1/S96421
SERIAL NO. 09/970,912
PATENT

In view of the foregoing, Applicant respectfully submits that Claims 1-21 are allowable and requests notice to that effect.

Further and favorable consideration is respectfully requested.

Respectfully submitted,

Date: 01/15/07

Madelynne J. Farber
Registration No. 45,410

Sandia National Laboratories
P.O. Box 5800, MS 0161
Albuquerque, NM 87185-0161
(p) 505-844-3858, (f) 505-844-9955